Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 03 November 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports an engineer has been arrested on charges that he sent off blueprints for critical nuclear−plant parts, knowing they might be headed for North Korea. (See item 1)
- CNN/Money reports that less than a month after the release of new $20 bills with features designed to deter forgeries, counterfeiters are already at work. (See item 6)
- The Associated Press reports the federal government says two Wisconsin companies have voluntarily recalled nearly 80 thousand pounds of beef over contamination fears of a deadly strain of E. coli. (See item 15)
- eSecurity Planet reports that Microsoft has issued major revisions to several critical security patches because of problems associated with Debug Programs. (See item 26)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *November 01, Associated Press* — **New Jersey man accused of sending nuke plans.** An engineer was arrested Friday, October 31, on charges that he sent off blueprints for critical nuclear−plant parts, knowing they might be headed for North Korea. A criminal complaint filed

in U.S. District Court in Manhattan accused Sitaraman Ravi Mahadevan of shipping blueprints for valves to Mitsubishi Heavy Industries Inc. in New York, knowing they might be sent to North Korea. **Mahadevan allegedly shipped six packages containing approximately 90 blueprints to Mitsubishi, one of the contractors responsible for constructing the Korean Peninsula Energy Development Organization's nuclear plant in North Korea, prosecutors said. Prosecutors said the export of the valves or their blueprints to any nuclear facility in North Korea without a valid government export license is prohibited.** An investigation by the Commerce Department, which issues export licenses, led to the seizure of the blueprints while they were en route to Mitsubishi.
Source: http://www.foxnews.com/story/0,2933,101901,00.html

2. *October 31, Associated Press* — **Pair gets 30 months in prison for vandalizing power lines.** Two Rock Springs, WY, men were each sentenced to 2 1/2 years in prison for knocking down power lines last March in southwest Wyoming. **The two admitted to loosening the guy wires to an Idaho Power Co. transmission tower, which fell and pulled down four other towers west of Green River, WY on March 30.** They had been drinking heavily that day. No customers lost power but the two caused $1,035,431 in damage.
Source: http://www.billingsgazette.com/index.php?tl=1&display=rednews/2003/10/31/build/wyoming/70−powerlines.inc

3. *October 31, Reuters* — **Sun storm causes problems for Swedish power system. The solar storm has caused technical glitches in Sweden's power system in the past few days and may be to blame for a blackout that affected 50,000 people on Thursday, October 30.** Magnetic solar storms can wreak havoc with electricity grids, and the effects continued to be felt on Friday, October 31, in the Nordic region, particularly in Sweden where problems with transformers at a nuclear station and in the grid were observed, officials said. Power was cut around 9 p.m. on Thursday in the southern Sweden city of Malmo and lasted 20 minutes to a half hour, utility Sydkraft said in a statement. "We have not 100 percent identified the solar storm as the cause, but it might have been," said Sydkraft official Peter Sigenstam. **A spokesperson for Sweden's national grid, Svenska Kraftnat said that two transformers had malfunctioned, but the problems were quickly fixed and had not caused power outages to consumers.**
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2003_10_31_eng−reuters_pma_SUN−STORM−CAUSES−PROBLEMS−FOR−SWEDISH−POWER−SYSTEM&SMContentSet=0

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4.

October 31, Aerospace Daily — **Defense equipment gets funding boost in war bill compromise. A House−Senate panel approved a fiscal 2004 supplemental appropriations conference report Wednesday, October 29, that provides tens of millions of dollars above the Bush Administration's request to buy aviation, communications and radio−jamming equipment.** Requests receiving full funding include $3.1 billion for classified Air Force procurement, $59.1 million for Navy aircraft spare parts, $13 million for Navy F/A−18 equipment, $8 million for the Army's RC−12 Guardrail aircraft, $6 million to repair the Navy's Advanced Tactical Air Reconnaissance System (ATARS), and $4.85 million for Air Force procurement of Hellfire missiles used on Predator unmanned aerial vehicles. A $10 million request to improve the Air Force's RC−135 Rivet Joint aircraft was denied on the grounds that it was not related to the Afghanistan and Iraq conflicts that the supplemental is supposed to fund. **The full House and Senate are expected to approve the supplemental within the next few days.**
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/war10313.xml

[Return to top]

Banking and Finance Sector

5. *October 31, News Interactive (Australia)* — **More scam banking spam in Australia.** Another fraudulent banking e−mail scam has emerged in Australia, this time targeting ANZ bank users. **The latest attack used bulk email messages, mostly sent Thursday, October 30, which appears to come from "antifraud@anz.com" and featured "Attention!" on the subject line.** As with most previous online banking scams, it urged customers to update their details for security reasons by clicking on a link which appeared to be anz.com, but actually resolves to another address. ANZ spokesperson Paul Edwards said **Australian Federal Police had been alerted and the site, which was hosted in the U.S., appears to have already been taken offline.**
Source: http://www.news.com.au/common/story_page/0,4057,7724757%255E 15306,00.html

6. *October 29, CNN/Money* — **Counterfeit new $20s debut. Less than a month after the release of new $20 bills with features designed to deter forgeries, counterfeiters are already at work.** Recently, people in and around Brockton, MA, tried to pass fake notes at a convenience store, a restaurant, and a Radio Shack, according to the Brockton police department. In an unrelated incident on Tuesday, October 28, phony bills showed up at a convenience store in Quincy, MA, according to Steve Ricciardi, Special Agent in charge of the Secret Service's Boston office. **The Massachusetts scams were not the only recently reported forgeries. In Indiana, at least five fake notes have been passed.** A restaurant in Elkhart, IN, found two of them. Three other counterfeit bills have also turned up in the Elkhart area in recent days, according to Tom Cutler, a lieutenant and spokesman for the Elkhart police. "All of them have been what I'd call 'sophisticated copies,' not ultra high−tech notes," he said. **In the case of the Elkhart forgeries, Cutler said that the color−shifting ink was obviously not present. In Massachusetts, too, the false notes lacked enhanced features.** "There was no security strip, no red−and−blue fibers in the paper, and the watermark was missing," said Ricciardi.
Source: http://money.cnn.com/2003/10/29/pf/debt/counterfeit_20_found /?cnn=yes

[Return to top]

Transportation Sector

7. *October 31, Portland Press Herald (ME)* — **Federal experts promise to increase port security. Federal security experts toured the Portland, ME, waterfront Thursday, October 30, and offered help to city officials trying to improve security around passenger ships.** "Everyone recognizes this has to be a cooperative effort," said Donald Thompson, director of the Maritime Passenger Security Branch of the U.S. Transportation Security Administration (TSA), during a tour of the International Marine Terminal. Jeff Monroe, the city's transportation and ports director, said the visit was a step toward better security and better collaboration. Neither Monroe nor the TSA officials would discuss any specifics of the security improvements they discussed Thursday. Officials in Portland and around the country are in the final phase of preparing seaport security plans that must be submitted to the Department of Homeland Security by the end of the year. **Monroe has said the city plans to be the first port in the nation to require cruise ship and ferry passengers to go through a screening process similar to the one used in airports.**
   Source: http://www.pressherald.com/news/local/031031portwaterfront.s html

8. *October 31, nbc4.com (DC)* — **Washington, DC officials state transportation infrastructures are security risk. An assessment of city officials who were asked to respond to a homeland security survey by the House Democratic Caucus discloses that the bridges and tunnels in the District of Columbia are so old that they might not be able to handle traffic during a rapid evacuation of the city. District of Columbia Delegate Eleanor Holmes Norton said about $300 million is needed to repair tunnels and bridges along major evacuation routes.** About one million people commute into the city each day, including about 200,000 federal workers. Although the District has received $156 million for homeland security projects in the past two years, much of the money has been spent on training and equipment for emergency service providers.
   Source: http://www.nbc4.com/news/2594706/detail.html

9. *October 30, U.S. Coast Guard* — **Security enhanced at Alaska's Valdez port. A high−tech infrared camera system now monitors the port of Valdez and vessels transiting Prince William Sound in Alaska.** This infrared maritime surveillance system supplements the extensive maritime and land−based homeland security measures put in to action in Valdez and around the nation following the events of September 11, 2001. The cameras, capable of seeing through the rain, fog, snow and darkness, detect minute differences in surface temperatures. **Monitors and camera controls for the system are located at the Valdez Police department, the Coast Guard Vessel Traffic Services center, ALYESKA− Ship Escort and Response Vessel Services (SERVS) and also at the Alyeska marine terminal.** This system greatly enhances the Coast Guard and other members of the Valdez port security committee's ability to discern objects and details impossible to see with the naked eye and existing radar systems.
   Source: http://www.uscg.mil/d17/allnews/news03/20703.htm

10. *October 30, U.S. Coast Guard* — **Marine security act finalized.** The final rule for the Marine Transportation Security Act was published in the Code of Federal Register October 22. **These**

regulations significantly strengthen the security of U.S. ports by requiring preventative security measures and plans to deter threats and provide a framework for response in the event of an attack. By requiring completion of security assessments, development of security plans, and implementation of security measures and procedures, these regulations will reduce the risk and mitigate the exposure of our ports and waterways to terrorist activity. **The security regulations focus on those sectors of maritime industry that have a higher risk of involvement in a transportation security incident, including various tank vessels, barges, large passenger vessels, cargo vessels, towing vessels offshore oil and gas platforms, and port facilities that handle certain kinds of dangerous cargo or service the vessels listed above.** Security plans are required for all vessels and facilities, with minor exceptions. To promote innovation and flexibility, the Department of Homeland Security is also encouraging the private sector to develop acceptable alternatives to accommodate specific security measures.
Source: http://www.uscg.mil/d17/allnews/news03/20603.htm

[Return to top]

Postal and Shipping Sector

11. *October 31, DM News* — **Mail deliveries rebound as California wildfires lessen.** Mail service is slowly returning to normal in Southern California after the wildfires there this week prevented the U.S. Postal Service (USPS) from making more than 1 million deliveries in the Van Nuys, Santa Ana, and San Diego postal districts. **As of Thursday, full delivery service had resumed in the Van Nuys and Santa Ana districts, but the San Bernardino Mountains and the city of San Diego in the San Diego District still were experiencing delays, including the closure of 15 post offices in the San Bernardino Mountains.** USPS spokesman David Mazer said that only several hundred deliveries were not made Thursday. The USPS set up temporary post offices in San Bernardino and San Diego County where residents can pick up their mail. **United Parcel Service (UPS) is also getting back on schedule after being hard hit at the start of the week.** "The biggest impact was Monday and part of Tuesday," UPS spokesman Bob Godlewski said. "But it is still not perfect yet. Things are moving, but there may be delays." Godlewski said that UPS was particularly concerned that railroad service in the area has been shut down since Sunday. **A FedEx spokesman said that most of its package delivery has been unaffected.**
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2545 7

[Return to top]

Agriculture Sector

12. *October 31, Iowa Ag Connection* — **Cattle rustlers at work in West Virginia. At least three West Virginia livestock farms have reported missing cattle in recent weeks, and the state Department of Agriculture is urging farmers to lock their gates and watch for strangers.** "You can turn cattle loose and they wander around the hills," agency spokesman Buddy Davidson said Tuesday. "You've got cattle out in the fields, and particularly in West Virginia, when they're up over the ridge, they're out of sight. People can just back in and load them up."

West Virginia has about 405,000 head of cattle and some 11,000 beef farmers, Davidson said. That amounts to a $240 million industry, second in size only to poultry. **"Cattle prices have reached record levels, and that may be tempting some individuals to take cattle that doesn't belong to them," Commissioner of Agriculture Gus Douglass said.** A single unslaughtered cow could be worth as much as $1,000 to a thief, agricultural officials say. **In the past year, beef prices have risen from 85 to 90 cents per pound to as much as $1.20.**
Source: http://www.iowaagconnection.com/story−state.cfm?Id=861&yr=20 03

13. *October 31, University of California, Berkeley* — **Mapping of plant genome could lead to new of hybrid plants.** In a study led by researchers at the University of California, Berkeley, and the Salk Institute, scientists have accurately mapped the genes of the common mustard weed, Arabidopsis. **The achievement may lead to the next generation of genetically modified crops that can grow faster, produce more food, and resist disease. The study reveals the existence of nearly 6,000 genes, about one−third of the genes that exist in Arabidopsis.** Knowing these genes and how they work can allow researchers, in a short period of time, to use them to change the characteristics of other plants. "Arabidopsis has all the genes a plant needs," said Joe Ecker, Salk professor of plant biology. "All flowering plants are closely related, and so the genes that encode various traits are also shared. It's possible, then, to take a gene for flowering from Arabidopsis and insert it into rice or poplar, and have that gene function." **The findings revealed some shortcomings of computer−based gene prediction programs.** Computer programs may still put genes' parts in the wrong places, find genes that aren't really there, or miss genes altogether.
Source: http://www.sciencedaily.com/releases/2003/10/031031063921.ht m

14. *October 31, AgWeb* — **Proposed rule on imports of Canadian cattle. U.S. Department of Agriculture (USDA) Friday issued a proposed rule to amend its bovine spongiform encephalopathy (BSE) regulations to establish a new category of regions that recognizes those that present a minimal risk of introducing BSE into the U.S. via the importation of certain low−risk live ruminants and ruminant products.** USDA's Animal and Plant Health Inspection Service (APHIS) is seeking public comment on the proposal to allow the importation of certain live ruminants and ruminant products and byproducts from minimal risk regions under specified conditions. This proposed rule would place Canada on a list of countries considered a minimal risk for BSE. **The proposed minimal risk region would include regions in which an animal has been diagnosed with BSE but in which specific preventive measures have been in place for an appropriate period of time that reduce the risk of BSE being introduced to the United States.** Based on a comprehensive risk analysis and review, USDA believes that the surveillance, prevention, and control measures implemented by Canada are sufficient to be included in the minimal risk category.
Source: http://www.agweb.com/news_show_news_article.asp?file=AgNewsA rticle_200310311512_5636&articleid=102632&newscat=GN

[Return to top]

Food Sector

15. *November 02, Associated Press* — **Wisconsin companies recall beef. The federal government says two Wisconsin companies voluntarily recalled nearly 80 thousand**

pounds of beef Saturday over contamination fears. Abbyland Meats, of Abbotsford, sold about 78 thousand pounds of fresh boneless beef to wholesalers in Wisconsin, Minnesota, Ohio, Illinois, and Pennsylvania. The second company's meat was sold to restaurants in Wisconsin. **The U.S. Department of Agriculture's (USDA) Food and Safety Inspection Service says the companies learned the meat may have been contaminated with a deadly strain of E. coli.** The USDA said it had not received any reports of illness connected with the meat products. The strain of bacteria can cause severe diarrhea, dehydration, and even death. Source: http://www.wpxi.com/news/2603365/detail.html

[Return to top]

Water Sector

16. *October 31, Wood TV Channel 8* — **Break−in at Grand Rapids water pumping station. A Grand Rapids, MI, water official says security concerns will be addressed today following a break−in at a city pumping station Thursday night.** It happened at 9:30 p.m. City Water Assistant Mananger Don Spencer says an alarm system was tripped after someone kicked in a vent. Nothing was taken or vandalized. **Spencer says police responded quickly, and that the city's water supply was never at any risk of contamination because the station is shut down at night. He says earlier this year, the utility went through an extensive security assesment thanks to a grant from the U.S. Environmental Protection Agency.** Source: http://www.woodtv.com/Global/story.asp?S=1505394&nav=0RceIqB F

[Return to top]

Public Health Sector

17. *October 31, Associated Press* — **Vaccine−evading mousepox virus created.** A research team backed by a federal grant has created a genetically engineered mousepox virus designed to evade vaccines, highlighting the deadly potential of biotechnology and bioterrorism. **The team at St. Louis University, led by Mark Buller, created the superbug to figure out how to defeat it, a key goal of the government's anti−terrorism plan.** Researchers designed a two−drug cocktail that promises to defeat their exceptionally deadly virus. "The whole focus was to contribute to the biodefense agenda of the country," Buller said. Buller spliced a gene known to suppress the immune system into the mousepox virus, then injected the combined strand into vaccinated mice. All of them died. **Buller said infected mice recovered when treated with a combination of anti−viral drugs, providing hope that a treatment against genetically engineered smallpox could be developed. Mousepox can't be passed to humans, but it's a close relative to smallpox, making it an ideal virus to study in animals.** When Buller presented his results last week at an international biodefense conference, it prompted debate among some attendees. Some feared that publication of such information could help terrorists create biological weapons laced with genetically modified superbugs. Such germs are created by splicing drug−resistant genes in viruses normally defeated by vaccines. Source: http://www.theledger.com/apps/pbcs.dll/article?AID=/20031031 /APF/310310548

18.

October 31, Reuters — **U.S. short of trained epidemiologists.** Almost half of the epidemiologists working in state health departments in the U.S. have no training in their area of specialty, according to a survey that raises questions about the nation's ability to face a range of public health threats. **Increasing the number of state, local, and tribal health departments that have the staff and resources to properly investigate public health problems is one of the federal government's national health objectives for 2010. But a national survey by the Council of State and Territorial Epidemiologists indicates that the nation has a long way to go before this goal is attained. A total of 787 health department epidemiologists, or 42 percent of those surveyed in 41 states and three U.S. territories, said they had never completed coursework or other formal training in the field, according to the survey.** Only a few states and territories reported having full or near−full capacity to maintain surveillance of emerging health crises, such as bioterrorism attacks or environmental disasters. Dr. Matthew Boulton, a member of the survey team, noted that a renewed interest and increase in funding for public health during the past two years made him optimistic that the nation was addressing the training gap in epidemiology.
Source: http://www.reuters.com/newsArticle.jhtml?type=domesticNews&s toryID=3727316

19. *October 30, Milwaukee Journal Sentinel* — **Scientists reverse a fatal brain disease in mice.** By using genetic trickery, a group of British scientists has reversed a type of fatal brain disease, a finding that has implications for a family of deadly neurological disorders in people, cattle, and deer. **Researchers using laboratory mice say they were able to halt and actually reverse the disease process caused by an unusual infectious agent known as a prion. Prions are rogue proteins that attack the brain and are believed to be the cause of a family of diseases that includes Creutzfeldt−Jakob disease in people, mad cow disease, and chronic wasting disease in deer.** People also can be infected with the human version of mad cow disease, called variant Creutzfeldt−Jakob disease. **The approach by the British group represents a revolutionary way of curing otherwise incurable diseases: Instead of seeking out and destroying the infectious agent, which is the conventional approach with invading viruses and bacteria, they have focused on the target of the agent.** The researchers were able to halt the advance of prion disease essentially by eliminating a normal protein in the brain that is infected by prions.
Source: http://www.centredaily.com/mld/centredaily/news/7144496.htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

20. *October 31, NASA/Goddard Space Flight Center* — **Earth alert system to aid in disasters.** The Maryland Emergency Management Agency (MEMA) has recently deployed a new communications system, based on NASA technology, that is designed to aid emergency management professionals when natural or man−made disasters occur. **During the early hours**

of Hurricane Isabel, key Maryland Emergency Management officials had access to Earth Alert, a system that enabled MEMA to quickly view personnel deployment and status on a map, track personnel movement, send text alerts, as well as send messages to and from devices in the field. They were also able to report damages and coordinate response teams operating in the field. During a one−year pilot program, MEMA officials are testing the Earth Alert Emergency Management System. The development of the Earth Alert System is based on NASA Goddard's communications and information systems technologies. **Because Earth Alert is a hosted Web−based solution, it can be implemented without buying expensive call center infrastructure, networked computer servers, or special hardware for field deployment.**
Source: http://www.sciencedaily.com/releases/2003/10/031030062554.ht m

21. *October 31, General Accounting Office* — **Report−GAO−04−72: Overview of Federal Disaster Assistance to the New York City Area.** The federal government has been a key participant in the efforts to provide aid to the New York City area to help it respond to and recover from the September 11 terrorist attacks. The President pledged, and the Congress subsequently authorized, about $20 billion in federal aid. **This federal aid was provided primarily through four sources: the Federal Emergency Management Agency (FEMA), the Department of Housing and Urban Development (HUD), the Department of Transportation (DOT), and the Liberty Zone tax benefits−a set of tax benefits targeted to lower Manhattan.** These sources provided 96 percent, or $19.63 billion, of the committed federal aid to the New York City area. It has been over two years since the attacks occurred, and many efforts have been undertaken to aid the New York City area to cope with the disaster and its many impacts. **GAO was asked to describe how much and what type of federal assistance was provided to the New York City area through these four sources and how the federal government's response to this disaster differed from previous disasters**.
Highlights: http://www.gao.gov/highlights/d0472high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−72

[Return to top]

Information and Telecommunications Sector

22. *October 31, Federal Computer Week* — **DHS rounds out science unit.** Supporting and anticipating the needs of its colleagues in the Department of Homeland Security (DHS) is the top priority for the now−complete Science and Technology Directorate, an official told the House Homeland Security Committee's Cybersecurity, Science, and Research and Development (R&D) Subcommittee last week. The directorate is almost fully staffed, with experts in all the lead positions, said Penrose Albright, assistant secretary for science and technology. Portfolio directors are also in place to ensure coordination among the pieces of DHS, with all near−, mid− and long−range research coordinated by the top staff at the Office of Plans, Programs and Budgets. **The directorate is developing a robust cybersecurity R&D center within the Homeland Security Advanced Research Projects Agency for the Information Analysis and Infrastructure Protection Directorate**, Albright said. **The center developed an agenda to examine many topics, such as understanding infrastructure vulnerabilities and detecting insider threats**. The directorate also is establishing technical standards with the National Institute of Standards and Technology for many areas, including

radiation detection standards and interoperable communications equipment.
Source: http://fcw.com/fcw/articles/2003/1027/web−dhs−10−31−03.asp

23. *October 30, CNET News.com* — **Broadband numbers show heightened demand.** After a quarter marked by DSL price cuts and cable speed boosts, one thing is clear: broadband use is surging, regardless of what form it takes. **Recently released numbers from cable companies and from the Baby Bells who provide digital subscriber line access make it plain the companies are watching their broadband Net businesses flourish.** It's unclear whether aggressive price cuts by DSL providers are eating into cable's market−share lead, or whether cable's doubling of its download speed has effectively countered the price cuts. But both sides know the fight for the remaining 80 percent of U.S. homes without broadband will intensify this quarter. Cable companies offer their own broadband services for between $45 and $55 a month with faster download speeds than DSL. Some companies have also begun to experiment with discount promotions, such as offering service for $29.95 a month for the first three months.
Source: http://news.com.com/2100−1034_3−5100321.html?tag=nefd_top

24. *October 30, FCC* — **FCC acts to speed broadband deployment in rural America.** The Federal Communications Commission (FCC) has released the agenda and further details for Rural Wireless Internet Service Provider Showcase and Workshop to be held at the Commission on November 4. **This event is part of ongoing Commission efforts intended to facilitate the deployment of broadband services in rural America**. Wireless ISPs (WISPs) have been sprouting up across rural America providing high−speed Internet access using both licensed and unlicensed spectrum. **Deploying networks which use grain elevators, water towers, and mountain tops as antenna sites, rural WISPs are beginning to bring broadband service to previously unserved areas and to provide new competition in areas that already have broadband access**. The Rural WISP Showcase will feature "virtual tours" of several WISPs, discussions of technology, implementation issues, best practices, and lessons learned. In addition, **it will provide an opportunity for the Commission to learn what, if any, regulatory barriers stand in the way of rural WISP deployment**. Additional information about the Showcase is available Online: http://www.fcc.gov/osp/rural−wisp.html
Source: http://www.fcc.gov/

25. *October 30, FCC* — **Media Security and Reliability Council to review infrastructure security recommendations.** Recommendations to ensure the continued operation and security of media infrastructure will be presented to leaders from the broadcast, cable and satellite industries at the biannual Media Security and Reliability Council (MSRC) meeting Thursday, November 6. MSRC is a Federal Advisory Committee that reports to FCC Chairman Michael K. Powell. **Chairman Powell formed MSRC following the events of September 11, 2001, in order to study, develop and report on best practices designed to assure the optimal reliability, robustness and security of the broadcast and multichannel video programming distribution industries**. The Communications Infrastructure Security, Access and Restoration Working Group will present detailed best practices recommendations relating to physical security, including prevention and restoration matters. The council members have until November 26 to vote on the recommendations.
Source: http://www.fcc.gov/

26.

October 30, eSecurity Planet — **Microsoft revises critical patches.** Microsoft has issued major revisions to several 'critical' security patches because of problems associated with Debug Programs. **The "major revisions" issued on October 30 have been released to correct problems in the MS03−042, MS03−043, and MS03−045 patches**. The MS03−042 patch, which plugs a 'critical' buffer overflow issue in the Windows Troubleshooter ActiveX Control, has been re−issued because of problems related to CPU resource usage. **The Debug Problems afflict all three faulty patches**−−MS03−043, which is a buffer overrun in Messenger Service that could lead to code execution and MS03−044, which could allow PC takeover because of buffer overflows in the ListBox and ComboBox Control. Additional information is available on the Microsoft Website: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/winoct03.asp
Source: http://www.esecurityplanet.com/prodser/article.php/3101901

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 445 (microsoft−ds), 1433 (ms−sql−s), 80 (www), 17300 (Kuang2TheVirus), 139 (netbios−ssn), 4662 (eDonkey2000), 27374 (SubSeven) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *November 02, New York Times* — **U.S. copter downed in Iraq, killing 15 and wounding 21. The Chinook helicopter was hit by a missile and exploded in midair in Falluja on Sunday, several witnesses in this farming community 40 miles west of Baghdad said. A second explosion followed when the helicopter hit the ground, they said. Another missile narrowly missed a second Chinook, the witnesses said. Their accounts matched descriptions of a shoulder−fired missile.** Guerrillas fired the missiles from a heavy grove of palm trees a few hundred yards north of the crash site, the witnesses said. The United States military said it could not confirm that a missile caused the crash. **The site of the crash is a farming community about five miles southwest of Falluja, a city where anti−American sentiment is high and residents clash almost every day with American soldiers.** In a

separate attack, an American convoy was bombed today in Falluja, destroying at least one armored vehicle. **Saddam Hussein's army had an arsenal of thousands of surface−to−air missiles. Most have not been accounted for, and guerrillas regularly fire missiles at military airplanes landing or taking off from Baghdad's airport, American military officials have said.**
Source: http://www.nytimes.com/2003/11/02/international/middleeast/02CND−IRAQ.html?ex=1068440400&en=d2f904f41fb9f00f&ei=5062&par tner=GOOGLE

28. *October 30, Associated Press* — **Indonesian police are warned of more attacks. Two men arrested for a hotel bombing in Jakarta, Indonesia, have admitted they were part of a Jemaah Islamiyah cell and warned it was planning more attacks,** police said Thursday, October 30. The two men, Tohir and Ismail, told police that the attacks were being coordinated by Azahari bin Husin, a top Jemaah Islamiyah leader from Malaysia who is wanted in the August 5 bombing at Jakarta's Marriott hotel and last year's Bali bombings. The suspects also said the group had at least 11 pounds of explosives at its disposal. **Police claim they prevented the two suspects from blowing themselves up when they surprised them at a hotel Wednesday, October 29, in the West Java town of Cirebon.** Also Thursday, police said they narrowly missed arresting Azahari and another key terror suspect, Noordin Mohammed Top, on Wednesday in the West Java provincial capital of Bandung. Police said they could have shot them as they ran from a rented house but feared the men would detonate bombs they supposedly had with them. **Lt. General Erwin Mapasseng said police later found four homemade bombs at the house, and Ismail told police the bombs were intended for a Citibank in Bangdung.**
Source: http://www.newsday.com/news/nationworld/world/wire/sns−ap−indonesia−terror−arrests,0,5374452.story?coll=sns−ap−world−hea dlines

29. *October 27, Los Angeles Police Department* — **LAPD advises homeowners to beware of firestorm scam−artists. The Los Angeles Police Department (LAPD) is advising all senior citizens to be extremely careful when strangers approach them regarding inspections of their residence due to the recent firestorms.** These scam−artists distract residents by asking if they can check the water pressure to ensure there is sufficient pressure to combat a fire, or they will want to check the rear yard to ensure that the trees are not a potential fire hazard. **While the resident is distracted, another suspect will enter the home and remove property and jewelry.** The LAPD wants to inform the public that water pressure is not checked from inside the residence and do not allow strangers into the rear yard to see if trees will present a fire hazard.
Source: http://www.lapdonline.org/press_releases/2003/10/PR03780.htm

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.